



Red Hat Virtualization 4.4

Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization 4.4 Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization Documentation Team

Red Hat Customer Content Services

rhev-docs@redhat.com

Legal Notice

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

A comprehensive guide to upgrading and updating components in a Red Hat Virtualization environment.

Table of Contents

RED HAT VIRTUALIZATION UPGRADE OVERVIEW	3
CHAPTER 1. UPGRADING A SELF-HOSTED ENGINE ENVIRONMENT	4
1.1. UPGRADING A SELF-HOSTED ENGINE FROM RED HAT VIRTUALIZATION 4.3 TO 4.4	4
1.2. UPGRADING A SELF-HOSTED ENGINE FROM RED HAT VIRTUALIZATION 4.2 TO 4.3	18
CHAPTER 2. UPGRADING A STANDALONE MANAGER LOCAL DATABASE ENVIRONMENT	32
2.1. UPGRADING FROM RED HAT VIRTUALIZATION 4.3 TO 4.4	32
2.2. UPGRADING FROM RED HAT VIRTUALIZATION 4.2 TO 4.3	52
CHAPTER 3. UPGRADING A STANDALONE MANAGER REMOTE DATABASE ENVIRONMENT	65
3.1. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM RED HAT VIRTUALIZATION 4.3 TO 4.4	65
3.2. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM RED HAT VIRTUALIZATION 4.2 TO 4.3	78
CHAPTER 4. UPDATES BETWEEN MINOR RELEASES	93
4.1. UPDATING RED HAT VIRTUALIZATION BETWEEN MINOR RELEASES	93
APPENDIX A. UPDATING THE LOCAL REPOSITORY FOR AN OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION	108
APPENDIX B. INSTALLING RHV HYPERVISORS FROM A LOCAL REPOSITORY	109
APPENDIX C. LEGAL NOTICE	111

RED HAT VIRTUALIZATION UPGRADE OVERVIEW

This guide explains how to upgrade the following environments to Red Hat Virtualization 4.3 or 4.4 :

- **Self-hosted engine, local database:** Both the Data Warehouse database and the Manager database are installed on the Manager.
- **Standalone manager, local database:** Both the Data Warehouse database and the Manager database are installed on the Manager.
- **Standalone manager, remote database:** Either the Data Warehouse database or the Manager database, or both, are on a separate machine.



NOTE

For a checklist of upgrade instructions, you can use the [RHV Upgrade Helper](#). This application asks you to fill in a checklist for your upgrade path and current environment, and presents the applicable upgrade steps.



IMPORTANT

Plan any necessary downtime in advance. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended VMs as soon as possible to apply the configuration changes.

Select the appropriate instructions for your environment from the following table. If your Manager and host versions differ (if you have previously upgraded the Manager but not the hosts), follow the instructions that match the Manager's version.

Table 1. Supported Upgrade Paths

Current Manager version	Target Manager version	Relevant section
4.3	4.4	<p>Self-hosted engine, local database environment: Upgrading a self-Hosted engine from Red Hat Virtualization 4.3 to 4.4</p> <p>Local database environment - Upgrading from Red Hat Virtualization 4.3 to 4.4</p> <p>Remote database environment: Upgrading a Remote Database Environment from Red Hat Virtualization 4.3 to 4.4</p>
4.2	4.3	<p>Self-hosted engine, local database environment: Upgrading a Self-Hosted Engine from Red Hat Virtualization 4.2 to 4.3</p> <p>Local database environment: Upgrading from Red Hat Virtualization 4.2 to 4.3</p> <p>Remote database environment: Upgrading a Remote Database Environment from Red Hat Virtualization 4.2 to 4.3</p>

CHAPTER 1. UPGRADING A SELF-HOSTED ENGINE ENVIRONMENT

1.1. UPGRADING A SELF-HOSTED ENGINE FROM RED HAT VIRTUALIZATION 4.3 TO 4.4

Upgrading a self-hosted engine environment from version 4.3 to 4.4 involves the following steps:

Upgrade Considerations

- When planning to upgrade, see [Red Hat Virtualization 4.4 upgrade considerations and known issues](#).
- When upgrading from Open Virtual Network (OVN) and Open vSwitch (OvS) 2.11 to OVN 2021 and OvS 2.15, the process is transparent to the user as long as the following conditions are met:
 - The Manager is upgraded first.
 - The ovirt-provider-ovn security groups must be disabled, before the host upgrade, for all OVN networks that are expected to work between hosts with OVN/OvS version 2.11.
 - The hosts are upgraded to match OVN version 2021 or higher and OvS version 2.15. You must complete this step in the Administration Portal, so you can properly reconfigure OVN and refresh the certificates.
 - The host is rebooted after an upgrade.



NOTE

To verify whether the provider and OVN were configured successfully on the host, check the **OVN configured** flag on the **General** tab for the host. If the **OVN Configured** is set to **No**, click **Management → Refresh Capabilities**. This setting is also available in the REST API. If refreshing the capabilities fails, you can configure OVN by reinstalling the host from Manager 4.4 or higher.

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool and Image Discrepancies tool to check for issues that might prevent a successful upgrade](#)
3. [Migrate any virtual machines that are running on the same host as the Manager virtual machine to another host in the same cluster](#)
4. [Place the environment in global maintenance mode](#)
5. [Update the 4.3 Manager to the latest version of 4.3](#)
6. [Upgrade the Manager from 4.3 to 4.4](#)
7. [Upgrade the self-hosted engine nodes, and any standard hosts, while reducing virtual machine downtime](#)
8. [\(Optional\) Upgrade RHVH while preserving local storage](#)

9. [Update the compatibility version of the clusters](#)
10. [Reboot any running or suspended virtual machines to update their configuration](#)
11. [Update the compatibility version of the data centers](#)

1.1.1. Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- When upgrading Red Hat Virtualization Manager, it is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

1.1.2. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

1.1.3. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

1.1.3.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.



NOTE

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
  storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
  storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  No discrepancies found
```

1.1.4. Migrating virtual machines from the self-hosted engine host

Only the Manager virtual machine should remain on the host until after you have finished upgrading the host. Migrate any virtual machines other than the Manager virtual machine to another host in the same cluster.

You can use Live Migration to minimize virtual machine down-time. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide* for more information.

1.1.5. Enabling global maintenance mode

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in global maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in global maintenance mode.

You can now update the Manager to the latest version of 4.3.

1.1.6. Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3.
Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt\*setup\* rh\*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

**NOTE**

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```

**IMPORTANT**

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.4.

1.1.7. Upgrading the Red Hat Virtualization Manager from 4.3 to 4.4

The Red Hat Virtualization Manager 4.4 is only supported on Red Hat Enterprise Linux versions 8.2 to 8.6. You need to do a clean installation of Red Hat Enterprise Linux 8.6, or Red Hat Virtualization Host on the self-hosted engine host, even if you are using the same physical machine that you use to run the RHV 4.3 self-hosted engine.

The upgrade process requires restoring Red Hat Virtualization Manager 4.3 backup files onto the Red Hat Virtualization Manager 4.4 virtual machine.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3.
- All virtual machines in the environment must have the cluster compatibility level set to version 4.3.
- Make note of the MAC address of the self-hosted engine if you are using DHCP and want to use the same IP address. The deploy script prompts you for this information.

- During the deployment you need to provide a new storage domain for the Manager machine. The deployment script renames the 4.3 storage domain and retains its data to enable disaster recovery.
- Set the cluster scheduling policy to **cluster_maintenance** in order to prevent automatic virtual machine migration during the upgrade.

CAUTION

In an environment with multiple highly available self-hosted engine nodes, you need to detach the storage domain hosting the version 4.3 Manager after upgrading the Manager to 4.4. Use a dedicated storage domain for the 4.4 self-hosted engine deployment.

- If you use an external CA to sign HTTPS certificates, follow the steps in [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*. The backup and restore include the 3rd-party certificate, so you should be able to log in to the Administration portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works. See [BZ#1313379](#) for more information.



NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Procedure

1. Log in to the Manager virtual machine and shut down the engine service.

```
# systemctl stop ovirt-engine
```

2. Back up the Red Hat Virtualization Manager 4.3 environment.

```
# engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
```

3. Copy the backup file to a storage device outside of the RHV environment.
4. Shut down the self-hosted engine.

```
# shutdown
```



NOTE

If you want to reuse the self-hosted engine virtual machine to deploy the Red Hat Virtualization Manager 4.4, note the MAC address of the self-hosted engine network interface before you shut it down.

5. Make sure that the self-hosted engine is shut down.

```
# hosted-engine --vm-status | grep -E 'Engine status|Hostname'
```

**NOTE**

If any of the hosts report the **detail** field as **Up**, log in to that specific host and shut it down with the **hosted-engine --vm-shutdown** command.

6. Install RHVH 4.4 or Red Hat Enterprise Linux 8.6 on the existing node currently running the Manager virtual machine to use it as the self-hosted engine deployment host. See [Installing the Self-hosted Engine Deployment Host](#) for more information.

**NOTE**

It is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

7. Install the self-hosted engine deployment tool.

```
# yum install ovirt-hosted-engine-setup
```

8. Copy the backup file to the host.

9. Log in to the Manager host and deploy the self-hosted engine with the backup file:

```
# hosted-engine --deploy --restore-from-file=/path/backup.bck
```

**NOTE**

tmux enables the deployment script to continue if the connection to the server is interrupted, so you can reconnect and attach to the deployment and continue. Otherwise, if the connection is interrupted during deployment, the deployment fails.

To run the deployment script using **tmux**, enter the **tmux** command before you run the deployment script:

```
# tmux
# hosted-engine --deploy --restore-from-file=backup.bck
```

The deployment script automatically disables global maintenance mode and calls the HA agent to start the self-hosted engine virtual machine. The upgraded host with the 4.4 self-hosted engine reports that HA mode is active, but the other hosts report that global maintenance mode is still enabled as they are still connected to the old self-hosted engine storage.

10. Detach the storage domain that hosts the Manager 4.3 machine. For details, see [Detaching a Storage Domain from a Data Center](#) in the *Administration Guide*.
11. Log in to the Manager virtual machine and shut down the engine service.

```
# systemctl stop ovirt-engine
```

12. Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4.

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

13. Install optional extension packages if they were installed on the Red Hat Virtualization Manager 4.3 machine.

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc
```



NOTE

The **ovirt-engine-extension-aaa-ldap** is deprecated. For new installations, use Red Hat Single Sign On. For more information, see [Installing and Configuring Red Hat Single Sign-On](#) in the *Administration Guide*.



NOTE

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

14. Configure the Manager by running the **engine-setup** command:

```
# engine-setup
```

The Red Hat Virtualization Manager 4.4 is now installed, with the cluster compatibility version set to 4.2 or 4.3, whichever was the preexisting cluster compatibility version.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

1.1.8. Migrating hosts and virtual machines from RHV 4.3 to 4.4

You can migrate hosts and virtual machines from Red Hat Virtualization 4.3 to 4.4 such that you minimize the downtime of virtual machines in your environment.

This process requires migrating all virtual machines from one host so as to make that host available to upgrade to RHV 4.4. After the upgrade, you can reattach the host to the Manager.



WARNING

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.



NOTE

CPU-passthrough virtual machines might not migrate properly from RHV 4.3 to RHV 4.4.

RHV 4.3 and RHV 4.4 are based on RHEL 7 and RHEL 8, respectively, which have different kernel versions with different CPU flags and microcodes. This can cause problems in migrating CPU-passthrough virtual machines.

Prerequisites

- Hosts for RHV 4.4 require Red Hat Enterprise Linux versions 8.2 to 8.6. A clean installation of Red Hat Enterprise Linux 8.6, or Red Hat Virtualization Host 4.4 is required, even if you are using the same physical machine that you use to run hosts for RHV 4.3.
- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the hosts belong is set to 4.2 or 4.3. All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.

Procedure

1. Pick a host to upgrade and migrate that host's virtual machines to another host in the same cluster. You can use Live Migration to minimize virtual machine downtime. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide*.
2. Put the host into maintenance mode and remove the host from the Manager. For more information, see [Removing a Host](#) in the *Administration Guide*.
3. Install Red Hat Enterprise Linux 8.6, or RHVH 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
4. Install the appropriate packages to enable the host for RHV 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
5. Add this host to the Manager, assigning it to the same cluster. You can now migrate virtual machines onto this host. For more information, see [Adding Standard Hosts to the Manager](#) in one of the *Installing Red Hat Virtualization* guides.

Repeat these steps to migrate virtual machines and upgrade hosts for the rest of the hosts in the same cluster, one by one, until all are running Red Hat Virtualization 4.4.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)
- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

1.1.9. Upgrading RHVH while preserving local storage

Environments with local storage cannot migrate virtual machines to a host in another cluster because the local storage is not shared with other storage domains. To upgrade RHVH 4.3 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain

in the 4.4 environment, and import the previous local storage into the new domain.

Prerequisites

- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the host belongs is set to 4.2 or 4.3.

Procedure

1. Ensure that the local storage on the RHVH 4.3 host's local storage is in maintenance mode before starting this process. Complete these steps:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the **Details** pane and select the storage domain in the results list.
 - c. Click **Maintenance**.
2. Reinstall the Red Hat Virtualization Host, as described in [Installing Red Hat Virtualization Host](#) in the *Installation Guide*.



IMPORTANT

When selecting the device on which to install RHVH from the **Installation Destination** screen, do not select the device(s) storing the virtual machines. Only select the device where the operating system should be installed.

If you are using Kickstart to install the host, ensure that you preserve the devices containing the virtual machines by adding the following to the Kickstart file, replacing ``device`` with the relevant device.

```
# clearpart --all --drives=device
```

For more information on using Kickstart, see [Kickstart references](#) in *Red Hat Enterprise Linux 8 Performing an advanced RHEL installation*.

3. On the reinstalled host, create a directory, for example **/data** in which to recover the previous environment.

```
# mkdir /data
```

4. Mount the previous local storage in the new directory. In our example, **/dev/sdX1** is the local storage:

```
# mount /dev/sdX1 /data
```

5. Set the following permissions for the new directory.

```
# chown -R 36:36 /data
# chmod -R 0755 /data
```

6. Red Hat recommends that you also automatically mount the local storage via **/etc/fstab** in case the server requires a reboot:

```
# blkid | grep -i sdX1
/dev/sdX1: UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" TYPE="ext4"
# vi /etc/fstab
UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" /data ext4 defaults 0 0
```

7. In the Administration Portal, create a data center and select **Local** in the **Storage Type** drop-down menu.
8. Configure a cluster on the new data center. See [Creating a New Cluster](#) in the *Administration Guide* for more information.
9. Add the host to the Manager. See [Adding Standard Hosts to the Red Hat Virtualization Manager](#) in one of the *Installing Red Hat Virtualization* guides for more information.
10. On the host, create a new directory that will be used to create the initial local storage domain. For example:

```
# mkdir -p /localfs
# chown 36:36 /localfs
# chmod -R 0755 /localfs
```

11. In the Administration Portal, open the **Storage** tab and click **New Domain** to create a new local storage domain.
12. Set the name to **localfs** and set the path to **/localfs**.
13. Once the local storage is active, click **Import Domain** and set the domain's details. For example, define **Data** as the name, **Local on Host** as the storage type and **/data** as the path.
14. Click **OK** to confirm the message that appears informing you that storage domains are already attached to the data center.
15. Activate the new storage domain:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the details pane and select the new data storage domain in the results list.
 - c. Click **Activate**.
16. Once the new storage domain is active, import the virtual machines and their disks:
 - a. In the **Storage** tab, select **data**.
 - b. Select the **VM Import** tab in the details pane, select the virtual machines and click **Import**. See [Importing Virtual Machines from a Data Domain](#) in the *Virtual Machine Management Guide* for more details.
17. Once you have ensured that all virtual machines have been successfully imported and are functioning properly, you can move **localfs** to maintenance mode.
18. Click the **Storage** tab and select **localfs** from the results list.

- a. Click the **Data Center** tab in the details pane.
- b. Click Maintenance, then click **OK** to move the storage domain to maintenance mode.
- c. Click **Detach**. The Detach Storage confirmation window opens.
- d. Click **OK**.

You have now upgraded the host to version 4.4, created a new local storage domain, and imported the 4.3 storage domain and its virtual machines.

1.1.10. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to 4.6 on the virtual machine and verifying the network connection.
If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

1.1.11. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute → Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

1.1.12. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

1.2. UPGRADING A SELF-HOSTED ENGINE FROM RED HAT VIRTUALIZATION 4.2 TO 4.3

Upgrading a self-hosted engine environment from version 4.2 to 4.3 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool and Image Discrepancies tool to check for issues that might prevent a successful upgrade](#)
3. [Place the environment in global maintenance mode](#)
4. [Update the 4.2 Manager to the latest version of 4.2](#)
5. [Upgrade the Manager from 4.2 to 4.3](#)
6. [Disable global maintenance mode](#)
7. [Upgrade the self-hosted engine nodes, and any standard hosts](#)
8. [Update the compatibility version of the clusters](#)
9. [Reboot any running or suspended virtual machines to update their configuration](#)
10. [Update the compatibility version of the data centers](#)
11. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

1.2.1. Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- When upgrading Red Hat Virtualization Manager, it is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

1.2.2. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

1.2.3. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

1.2.3.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

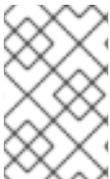
- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.



NOTE

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
  storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
  storage(5424252928) and on DB(5424254976)
```

```

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
No discrepancies found

```

1.2.4. Enabling global maintenance mode

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in global maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in global maintenance mode.

1.2.5. Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt\*setup\* rh\*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

Execution of setup completed successfully



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

1.2.6. Upgrading the Red Hat Virtualization Manager from 4.2 to 4.3

You need to be logged into the machine that you are upgrading.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to restore your Red Hat Virtualization Manager installation to its previous state. For this reason, do not remove the previous version's repositories until after the upgrade is complete. If the upgrade fails, the **engine-setup** script explains how to restore your installation.

Procedure

- Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

2. Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

3. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

4. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms
```

5. Update the base operating system:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

The Manager is now upgraded to version 4.3.

1.2.7. Disabling global maintenance mode

Procedure

1. Log in to the Manager virtual machine and shut it down.
2. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

3. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

-

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```



NOTE

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

1.2.8. Updating All Hosts in a Cluster

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See [oVirt Cluster Upgrade](#) for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:

- **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that are affected.
 7. Click **Upgrade**.
 8. A cluster upgrade status screen displays with a progress bar showing the percentage of completion, and a list of steps in the upgrade process that have completed. You can click **Go to Event Log** to open the log entries for the upgrade. Closing this screen does not interrupt the upgrade process.

You can track the progress of host updates:

- in the **Compute** → **Clusters** view, the **Upgrade Status** column displays a progress bar that displays the percentage of completion.
- in the **Compute** → **Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute** → **Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

1.2.9. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to 4.6 on the virtual machine and verifying the network connection. If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

1.2.10. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.

2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

1.2.11. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

1.2.12. Replacing SHA-1 Certificates with SHA-256 Certificates

Red Hat Virtualization 4.4 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures.

**WARNING**

Do *NOT* let certificates expire. If they expire, the environment becomes non-responsive and recovery is an error prone and time consuming process. For information on renewing certificates, see [Renewing certificates before they expire](#) in the *Administration Guide*.

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

5. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
      -nameopt compat \
    | sed \
      's;subject=(.*)\;1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \ <1> \
    --subject="${subject}" \
```

```

--san=DNS:"${ENGINE_FQDN}" \
--keep-key
done

```

Do not change this the password value.

- Restart the **httpd** service:

```
# systemctl restart httpd
```

- Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

- Log in to the Manager machine as the root user.
- Check whether **/etc/pki/ovirt-engine/openssl.conf** includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

- Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S)"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

- Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

- Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

6. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

7. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
      -nameopt compat \
    | sed \
      's;subject=\.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \ <1>
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

Do not change this the password value.

8. Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio
```

9. Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

10. Connect to the Administration Portal to confirm that the warning no longer appears.
11. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate

authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

12. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance** and **OK**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

CHAPTER 2. UPGRADING A STANDALONE MANAGER LOCAL DATABASE ENVIRONMENT

2.1. UPGRADING FROM RED HAT VIRTUALIZATION 4.3 TO 4.4

Upgrading your environment from 4.3 to 4.4 involves the following steps:

Upgrade Considerations

- When planning to upgrade, see [Red Hat Virtualization 4.4 upgrade considerations and known issues](#).
- When upgrading from Open Virtual Network (OVN) and Open vSwitch (OvS) 2.11 to OVN 2021 and OvS 2.15, the process is transparent to the user as long as the following conditions are met:
 - The Manager is upgraded first.
 - The `ovirt-provider-ovn` security groups must be disabled, before the host upgrade, for all OVN networks that are expected to work between hosts with OVN/OvS version 2.11.
 - The hosts are upgraded to match OVN version 2021 or higher and OvS version 2.15. You must complete this step in the Administration Portal, so you can properly reconfigure OVN and refresh the certificates.
 - The host is rebooted after an upgrade.



NOTE

To verify whether the provider and OVN were configured successfully on the host, check the **OVN configured** flag on the **General** tab for the host. If the **OVN Configured** is set to **No**, click **Management** → **Refresh Capabilities**. This setting is also available in the REST API. If refreshing the capabilities fails, you can configure OVN by reinstalling the host from Manager 4.4 or higher.

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool and Image Discrepancies tool to check for issues that might prevent a successful upgrade](#)
3. [Update the 4.3 Manager to the latest version of 4.3](#)
4. [Upgrade the Manager from 4.3 to 4.4](#)
5. [Migrate hosts and virtual machines while reducing virtual machine downtime](#)
6. [\(Optional\) Upgrade RHVH while preserving local storage](#)
7. [Update the compatibility version of the clusters](#)
8. [Reboot any running or suspended virtual machines to update their configuration](#)
9. [Update the compatibility version of the data centers](#)

2.1.1. Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- When upgrading Red Hat Virtualization Manager, it is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

2.1.2. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

2.1.3. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

2.1.3.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.

**NOTE**

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```

Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  No discrepancies found

```

You can now update the Manager to the latest version of 4.3.

2.1.4. Updating the Red Hat Virtualization Manager**Prerequisites**

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.4.

2.1.5. Upgrading the Red Hat Virtualization Manager from 4.3 to 4.4

Red Hat Virtualization Manager 4.4 is only supported on Red Hat Enterprise Linux versions 8.2 to 8.6. You need to do a clean installation of Red Hat Enterprise Linux 8.6 and Red Hat Virtualization Manager 4.4, even if you are using the same physical machine that you use to run RHV Manager 4.3.

The upgrade process requires restoring Red Hat Virtualization Manager 4.3 backup files onto the Red Hat Virtualization Manager 4.4 machine.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3.
- All virtual machines in the environment must have the cluster compatibility level set to version 4.3.
- If you use an external CA to sign HTTPS certificates, follow the steps in [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*. The backup and restore include the 3rd-party certificate, so you should be able to log in to the Administration portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works. See [BZ#1313379](#) for more information.



NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Procedure

1. Log in to the Manager machine.
2. Back up the Red Hat Virtualization Manager 4.3 environment.

```
# engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
```

3. Copy the backup file to a storage device outside of the RHV environment.
4. Install Red Hat Enterprise Linux 8.6. See [Performing a standard RHEL installation](#) for more information.
5. Complete the steps to install Red Hat Virtualization Manager 4.4, including running the command **yum install rhvm**, but do not run **engine-setup**. See one of the *Installing Red Hat Virtualization* guides for more information.
6. Copy the backup file to the Red Hat Virtualization Manager 4.4 machine and restore it.

```
# engine-backup --mode=restore --file=backup.bck --provision-all-databases
```



NOTE

If the backup contained grants for extra database users, this command creates the extra users with random passwords. You must change these passwords manually if the extra users require access to the restored system. See <https://access.redhat.com/articles/2686731>.

7. Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.
8. Install optional extension packages if they were installed on the Red Hat Virtualization Manager 4.3 machine.

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc
```

**NOTE**

The **ovirt-engine-extension-aaa-ldap** is deprecated. For new installations, use Red Hat Single Sign On. For more information, see [Installing and Configuring Red Hat Single Sign-On](#) in the *Administration Guide*.

**NOTE**

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

9. Configure the Manager by running the **engine-setup** command:

```
# engine-setup
```

10. Decommission the Red Hat Virtualization Manager 4.3 machine if a different machine is used for Red Hat Virtualization Manager 4.4. Two different Managers must not manage the same hosts or storage.
11. Run **engine-setup** to configure the Manager.

```
# engine-setup
```

The Red Hat Virtualization Manager 4.4 is now installed, with the cluster compatibility version set to 4.2 or 4.3, whichever was the preexisting cluster compatibility version. Now you need to upgrade the hosts in your environment to RHV 4.4, after which you can change the cluster compatibility version to 4.4.

Additional resources

- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

You can now update the hosts.

2.1.6. Migrating hosts and virtual machines from RHV 4.3 to 4.4

You can migrate hosts and virtual machines from Red Hat Virtualization 4.3 to 4.4 such that you minimize the downtime of virtual machines in your environment.

This process requires migrating all virtual machines from one host so as to make that host available to upgrade to RHV 4.4. After the upgrade, you can reattach the host to the Manager.

**WARNING**

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

**NOTE**

CPU-passthrough virtual machines might not migrate properly from RHV 4.3 to RHV 4.4.

RHV 4.3 and RHV 4.4 are based on RHEL 7 and RHEL 8, respectively, which have different kernel versions with different CPU flags and microcodes. This can cause problems in migrating CPU-passthrough virtual machines.

Prerequisites

- Hosts for RHV 4.4 require Red Hat Enterprise Linux versions 8.2 to 8.6. A clean installation of Red Hat Enterprise Linux 8.6, or Red Hat Virtualization Host 4.4 is required, even if you are using the same physical machine that you use to run hosts for RHV 4.3.
- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the hosts belong is set to 4.2 or 4.3. All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.

Procedure

1. Pick a host to upgrade and migrate that host's virtual machines to another host in the same cluster. You can use Live Migration to minimize virtual machine downtime. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide*.
2. Put the host into maintenance mode and remove the host from the Manager. For more information, see [Removing a Host](#) in the *Administration Guide*.
3. Install Red Hat Enterprise Linux 8.6, or RHVH 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
4. Install the appropriate packages to enable the host for RHV 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
5. Add this host to the Manager, assigning it to the same cluster. You can now migrate virtual machines onto this host. For more information, see [Adding Standard Hosts to the Manager](#) in one of the *Installing Red Hat Virtualization* guides.

Repeat these steps to migrate virtual machines and upgrade hosts for the rest of the hosts in the same cluster, one by one, until all are running Red Hat Virtualization 4.4.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)
- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

2.1.7. Upgrading RHVH while preserving local storage

Environments with local storage cannot migrate virtual machines to a host in another cluster because the local storage is not shared with other storage domains. To upgrade RHVH 4.3 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain in the 4.4 environment, and import the previous local storage into the new domain.

Prerequisites

- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the host belongs is set to 4.2 or 4.3.

Procedure

1. Ensure that the local storage on the RHVH 4.3 host's local storage is in maintenance mode before starting this process. Complete these steps:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the **Details** pane and select the storage domain in the results list.
 - c. Click **Maintenance**.
2. Reinstall the Red Hat Virtualization Host, as described in [Installing Red Hat Virtualization Host](#) in the *Installation Guide*.



IMPORTANT

When selecting the device on which to install RHVH from the **Installation Destination** screen, do not select the device(s) storing the virtual machines. Only select the device where the operating system should be installed.

If you are using Kickstart to install the host, ensure that you preserve the devices containing the virtual machines by adding the following to the Kickstart file, replacing ``device`` with the relevant device.

```
# clearpart --all --drives=device
```

For more information on using Kickstart, see [Kickstart references](#) in *Red Hat Enterprise Linux 8 Performing an advanced RHEL installation*.

3. On the reinstalled host, create a directory, for example **/data** in which to recover the previous environment.

```
# mkdir /data
```

4. Mount the previous local storage in the new directory. In our example, **/dev/sdX1** is the local storage:

```
# mount /dev/sdX1 /data
```

5. Set the following permissions for the new directory.

```
# chown -R 36:36 /data
# chmod -R 0755 /data
```

6. Red Hat recommends that you also automatically mount the local storage via **/etc/fstab** in case the server requires a reboot:

```
# blkid | grep -i sdX1
/dev/sdX1: UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" TYPE="ext4"
# vi /etc/fstab
UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" /data ext4 defaults 0 0
```

7. In the Administration Portal, create a data center and select **Local** in the **Storage Type** drop-down menu.
8. Configure a cluster on the new data center. See [Creating a New Cluster](#) in the *Administration Guide* for more information.
9. Add the host to the Manager. See [Adding Standard Hosts to the Red Hat Virtualization Manager](#) in one of the *Installing Red Hat Virtualization* guides for more information.
10. On the host, create a new directory that will be used to create the initial local storage domain. For example:

```
# mkdir -p /localfs
# chown 36:36 /localfs
# chmod -R 0755 /localfs
```

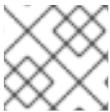
11. In the Administration Portal, open the **Storage** tab and click **New Domain** to create a new local storage domain.
12. Set the name to **localfs** and set the path to **/localfs**.
13. Once the local storage is active, click **Import Domain** and set the domain's details. For example, define **Data** as the name, **Local on Host** as the storage type and **/data** as the path.
14. Click **OK** to confirm the message that appears informing you that storage domains are already attached to the data center.
15. Activate the new storage domain:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the details pane and select the new data storage domain in the results list.
 - c. Click **Activate**.
16. Once the new storage domain is active, import the virtual machines and their disks:

- a. In the **Storage** tab, select **data**.
 - b. Select the **VM Import** tab in the details pane, select the virtual machines and click **Import**. See [Importing Virtual Machines from a Data Domain](#) in the *Virtual Machine Management Guide* for more details.
17. Once you have ensured that all virtual machines have been successfully imported and are functioning properly, you can move **localfs** to maintenance mode.
 18. Click the **Storage** tab and select **localfs** from the results list.
 - a. Click the **Data Center** tab in the details pane.
 - b. Click Maintenance, then click **OK** to move the storage domain to maintenance mode.
 - c. Click **Detach**. The Detach Storage confirmation window opens.
 - d. Click **OK**.

You have now upgraded the host to version 4.4, created a new local storage domain, and imported the 4.3 storage domain and its virtual machines.

2.1.8. Upgrading RHVH while preserving Gluster storage

Environments with Gluster as storage can take a backup of Gluster storage and be restored after the RHVH upgrade. Try to keep workloads on all virtual machines using Gluster storage as light as possible to shorten the time required to upgrade. If there are highly write-intensive workloads, expect more time to restore.



NOTE

GlusterFS Storage is deprecated, and will no longer be supported in future releases.

Prerequisites

- If there are geo-replication schedules on the storage domains, remove those schedules to avoid upgrade conflicts.
- No geo-replication sync are currently running.
- Additional disk space of 100 GB is required on 3 hosts for creating a new volume for the new RHVH 4.4 Manager deployment.
- All data centers and clusters in the environment must have a cluster compatibility level of 4.3 before you start the procedure.

Restriction

- Network-Bound Disk Encryption (NBDE) is supported only with new deployments with Red Hat Virtualization 4.4. This feature cannot be enabled during the upgrade.

Procedure

1. Create a new Gluster volume for RHVH 4.4 Manager deployment.

- a. Create a new brick on each host for the new RHVH 4.4 self-hosted engine virtual machine (VM).
- b. If you have a spare disk in the setup, follow the document [Create Volume](#) from the web console.
- c. If there is enough space for a new Manager 100GB brick in the existing Volume Group (VG), it can be used as a new Manager Logical Volume (LV).
Run the following commands on all the hosts, unless specified otherwise explicitly:

- d. Check the free size of the Volume Group (VG).

```
# vgdisplay <VG_NAME> | grep -i free
```

- e. Create one more Logical Volume in this VG.

```
# lvcreate -n gluster_lv_newengine -L 100G <EXISTING_VG>
```

- f. Format the new Logical Volume (LV) as XFS.

```
# mkfs.xfs <LV_NAME>
```

- g. Create the mount point for the new brick.

```
# mkdir /gluster_bricks/newengine
```

- h. Create an entry corresponding to the newly created filesystem in **/etc/fstab** and mount the filesystem.

- i. Set the SELinux Labels on the brick mount points.

```
# semanage fcontext -a -t glusterd_brick_t /gluster_bricks/newengine  
restorecon -Rv /gluster_bricks/newengine
```

- j. Create a new gluster volume by executing the gluster command on one of the hosts in the cluster:

```
# gluster volume create newengine replica 3 host1:/gluster_bricks/newengine/newengine  
host2:/gluster_bricks/newengine/newengine host3:/gluster_bricks/newengine/newengine
```

- k. Set the required volume options on the newly created volume. Run the following commands on one of the hosts in the cluster:

```
# gluster volume set newengine group virt  
gluster volume set newengine network.ping-timeout 30  
gluster volume set newengine cluster.granular-entry-heal enable  
gluster volume set newengine network.remote-dio off  
gluster volume set newengine performance.strict-o-direct on  
gluster volume set newengine storage.owner-uid 36  
gluster volume set newengine storage.owner-gid 36
```

- l. Start the newly created Gluster volume. Run the following command on one of the hosts in the cluster.

■

```
# gluster volume start newengine
```

2. Back up the Gluster configuration on all RHVH 4.3 nodes using the backup playbook.
 - a. The backup playbook is available with the latest version of RHVH 4.3. If this playbook is not available, create a playbook and inventory file:

```
/etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-deployment/archive_config.yml
```

Example:

```
all:
  hosts:
    host1:
    host2:
    host3:
  vars:
    backup_dir: /archive
    nbde_setup: false
    upgrade: true
```

- b. Edit the backup inventory file with correct details.

```
Common variables
backup_dir -> Absolute path to directory that contains the extracted contents of the
backup archive
nbde_setup -> Set to false as the {virt-product-fullname} 4.3 setup doesn't support
NBDE
upgrade -> Default value true . This value will make no effect with backup
```

- c. Switch to the directory and execute the playbook.

```
ansible-playbook -i archive_config_inventory.yml archive_config.yml --tags backupfiles
```

- d. The generated backup configuration tar file is generated under /root with the name **RHVH-
<HOSTNAME>-backup.tar.gz**. On all the hosts, copy the backup configuration tar file to the backup host.
3. Using the Manager Administration Portal, migrate the VMs running on the first host to other hosts in the cluster.
4. Backup Manager configurations.

```
# engine-backup --mode=backup --scope=all --file=<backup-file.tar.gz> --log=<logfile>
```

**NOTE**

Before creating a backup, do the following:

- Enable **Global Maintenance** for the self-hosted engine(SHE).
- Log in to the Manager VM using SSH and stop the ovirt-engine service.
- Copy the backup file from the self-hosted engine VM to the remote host.
- Shut down the Manager.

5. Check for any pending self-heal tasks on all the replica 3 volumes. Wait for the heal to be completed.

6. Run the following command on one of the hosts:

```
# gluster volume heal <volume> info summary
```

7. Stop the **glusterfs** brick process and unmount all the bricks on the first host to maintain file system consistency. Run the following on the first host:

```
# pkill glusterfsd; pkill glusterfs
# systemctl stop glusterd
# umount /gluster_bricks/*
```

8. Reinstall the host with RHVH 4.4 ISO, only formatting the OS disk.

**IMPORTANT**

Make sure that the installation does not format the other disks, as bricks are created on top of those disks.

9. Once the node is up following the RHVH 4.4 installation reboot, subscribe to RHVH 4.4 repos as outlined in the Installation Guide, or install the downloaded RHVH 4.4 appliance.

```
# yum install <appliance>
```

10. Disable the devices used for Gluster bricks.

- a. Create the new SSH private and public key pairs.
- b. Establish SSH public key authentication (passwordless SSH) to the same host, using frontend and backend network FQDN.
- c. Create the inventory file:

```
/etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-
deployment/blacklist_inventory.yml
```

Example:

```
hc_nodes:
hosts:
```

```
host1-backend-FQDN.example.com:
  blacklist_mpath_devices:
    - sda
    - sdb
```

- d. Run the playbook

```
ansible-playbook -i blacklist_inventory.yml
/etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-
deployment/tasks/gluster_deployment.yml --tags blacklistdevices*
```

11. Copy the Manager backup and host config tar files from the backup host to the newly installed host and untar the content using scp.
12. Restore the Gluster configuration files.
 - a. Extract the contents of the Gluster configuration files

```
# mkdir /archive
# tar -xvf /root/ovirt-host-host1.example.com.tar.gz -C /archive/
```

- b. Edit the inventory file to perform restoration of the configuration files. The Inventory file is available at **/etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-deployment/archive_config_inventory.yml**

Example playbook content:

```
all:
  hosts:
  host1.example.com:
  vars:
  backup_dir: /archive
  nbde_setup: false
  upgrade: true
```



IMPORTANT

Use only one host under 'hosts' section of restoration playbook.

- c. Execute the playbook to restore configuration files

```
ansible-playbook -i archive_config_inventory.yml archive_config.yml --tags restorefiles
```

13. Perform Manager deployment with the option **--restore-from-file** pointing to the backed-up archive from the Manager. This Manager deployment can be done interactively using the **hosted-engine --deploy** command, providing the storage corresponds to the newly created Manager volume. The same can also be done using **ovirt-ansible-hosted-engine-setup** in an automated procedure. The following procedure is an automated method for deploying a HostedEngine VM using the backup:
 - a. Create a playbook for HostedEngine deployment in the newly installed host:


```
/etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-deployment/he.yml
```

```
- name: Deploy oVirt hosted engine
```

```
hosts: localhost
roles:
  - role: ovirt.hosted_engine_setup
```

- b. Update the HostedEngine related information using the template file:
/etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-deployment/he_gluster_vars.json

Example:

```
# cat /etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-
deployment/he_gluster_vars.json

{
  "he_appliance_password": "<password>",
  "he_admin_password": "<password>",
  "he_domain_type": "glusterfs",
  "he_fqdn": "<hostedengine.example.com>",
  "he_vm_mac_addr": "<00:18:15:20:59:01>",
  "he_default_gateway": "<19.70.12.254>",
  "he_mgmt_network": "ovirtmgmt",
  "he_storage_domain_name": "HostedEngine",
  "he_storage_domain_path": "</newengine>",
  "he_storage_domain_addr": "<host1.example.com>",
  "he_mount_options": "backup-volfile-servers=<host2.example.com>:
<host3.example.com>",
  "he_bridge_if": "<eth0>",
  "he_enable_hc_gluster_service": true,
  "he_mem_size_MB": "16384",
  "he_cluster": "Default",
  "he_restore_from_file": "/root/engine-backup.tar.gz",
  "he_vcpus": 4
}
```

IMPORTANT

- In the above `he_gluster_vars.json`, There are 2 important values: `"he_restore_from_file"` and `"he_storage_domain_path"`. The first option `"he_restore_from_file"` should point to the absolute file name of the Manager backup archive copied to the local machine. The second option `"he_storage_domain_path"` should refer to the newly created Gluster volume.
- Also note that the previous version of RHVH Version running inside the Manager VM is down and that will be discarded. MAC Address and FQDN corresponding to the older Manager VM can be reused for the new Manager as well.

- c. For static Manager network configuration, add more options as listed below:

```
"he_vm_ip_addr": "<engine VM ip address>"
"he_vm_ip_prefix": "<engine VM ip prefix>"
"he_dns_addr": "<engine VM DNS server>"
"he_default_gateway": "<engine VM default gateway>"
```

**IMPORTANT**

If there is no specific DNS available, try to include 2 more options: "he_vm_etc_hosts": true and "he_network_test": "ping"

- d. Run the playbook to deploy HostedEngine Deployment.

```
# cd /etc/ansible/roles/gluster.ansible/playbooks/hc-ansible-deployment
# ansible-playbook he.yml --extra-vars "@he_gluster_vars.json"
```

- e. Wait for the self-hosted engine deployment to complete.

**IMPORTANT**

If there are any failures during self-hosted engine deployment, find the problem looking at the log messages under **/var/log/ovirt-hosted-engine-setup**, fix the problem. Clean the failed self-hosted engine deployment using the command **ovirt-hosted-engine-cleanup** and rerun the deployment.

14. Log in to the RHVH 4.4 Administration Portal on the newly installed Red Hat Virtualization manager. Make sure all the hosts are in the 'up' state, and wait for the self-heal on the Gluster volumes to be completed.

15. Upgrade the next host

- a. Move the next host (ideally, the next one in order), to Maintenance mode from the Administration Portal. Stop the Gluster service while moving this host to Maintenance mode.
- b. From the command line of the host, unmount Gluster bricks

```
# umount /gluster_bricks/*
```

- c. Reinstall this host with RHVH 4.4.

**IMPORTANT**

Make sure that the installation does not format the other disks, as bricks are created on top of those disks.

- d. If multipath configuration is not available on the newly installed host, disable the Gluster devices. The inventory file is already created in the first host as part of the step *Disable the devices used for Gluster bricks*.
 - i. Set up SSH public key authentication from the first host to the newly installed host.
 - ii. Update the inventory with the new host name.
 - iii. Execute the playbook.
- e. Copy the Gluster configuration tar files from the backup host to the newly installed host and untar the content.

- f. Restore Gluster configuration on the newly installed host by executing the playbook as described in the step *Restoring the Gluster configurations files* on this host.



IMPORTANT

Edit the playbook on the newly installed host and execute it as described in the step *Perform manager deployment with the option --restore-from-file...*. Do not change hostname and execute on the same host.

- g. Reinstall the host in RHVH Administration Portal Copy the authorized key from the first deployed host in RHVH 4.4

```
# scp root@host1.example.com:/root/.ssh/authorized_keys /root/.ssh/
```

- i. In the **Administration Portal**, The host will be in 'Maintenance'. Go to **Compute → Hosts → Installation → Reinstall**.
 - ii. In the **New Host** dialog box **HostedEngine** tab, and select the **deploy** self-hosted engine deployment action.
 - iii. Wait for the host to reach **Up** status.
- h. Make sure that there are no errors in the volumes related to GFID mismatch. If there are any errors, resolve them.

```
grep -i "gfid mismatch" /var/log/glusterfs/*
```

16. Repeat the step *Upgrade the next host* for all the RHVH in the cluster.
17. **(optional)** If a separate Gluster logical network exists in the cluster, attach the Gluster logical network to the required interface on each host.
18. Remove the old Manager storage domain. Identify the old Manager storage domain by the name **hosted_storage** with no gold star next to it, listed under **Storage → Domains**.
 - a. Go to the **Storage → Domains → hosted_storage → Data center** tab, and select **Maintenance**.
 - b. Wait for the storage domain to move into Maintenance mode.
 - c. Once the storage domain moves into Maintenance mode, click **Detach**, the storage domain will move to **unattached**.
 - d. Select the unattached storage domain, click **Remove**, and confirm **OK**.
19. Stop and remove the old Manager volume.
 - a. Go to **Storage → Volumes**, and select the old Manager volume. Click **Stop**, and confirm **OK**.
 - b. Select the same volume, click **Remove**, and confirm **OK**.
20. Update the cluster compatibility version.
 - a. Go to **Compute → Clusters** and select the cluster **Default**, click **Edit**, update the **Compatibility Version** to 4.4 and click **OK**.



IMPORTANT

There will be a warning for changing compatibility version, which requires VMs on the cluster to be restarted. Click **OK** to confirm.

21. There are new Gluster volume options available with RHVH 4.4, apply those volume options on all the volumes. Execute the following on one of the nodes in the cluster:

```
# for vol in gluster volume list; do gluster volume set $vol group virt; done
```

22. Remove the archives and extracted the contents of the backup configuration files on all nodes.

Creating an additional Gluster volume using the Web Console

1. Log in to the Manager web console.
2. Go to **Virtualization** → **Hosted Engine** and click **Manage Gluster**.
3. Click **Create Volume**. In the Create Volume window, do the following:
 - a. In the **Hosts** tab, select three different **ovirt-ng-nodes** with unused disks and click **Next**.
 - b. In the **Volumes** tab, specify the details of the volume you want to create and click **Next**.
 - c. In the **Bricks** tab, specify the details of the disks to be used to create the volume and click **Next**.
 - d. In the **Review** tab, check the generated configuration file for any incorrect information. When you are satisfied, click **Deploy**.

You can now update the cluster compatibility version.

2.1.9. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to 4.6 on the virtual machine and verifying the network connection. If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

You can now update the cluster compatibility version for virtual machines in the cluster.

2.1.10. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now update the data center compatibility version.

2.1.11. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

2.2. UPGRADING FROM RED HAT VIRTUALIZATION 4.2 TO 4.3

Upgrading your environment from 4.2 to 4.3 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool and Image Discrepancies tool to check for issues that might prevent a successful upgrade](#)
3. [Update the 4.2 Manager to the latest version of 4.2](#)
4. [Upgrade the Manager from 4.2 to 4.3](#)
5. [Update the hosts](#)
6. [Update the compatibility version of the clusters](#)
7. [Reboot any running or suspended virtual machines to update their configuration](#)
8. [Update the compatibility version of the data centers](#)
9. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

2.2.1. Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).

- When upgrading Red Hat Virtualization Manager, it is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

2.2.2. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

2.2.3. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

2.2.3.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.



NOTE

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```

Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  No discrepancies found

```

2.2.4. Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt-*setup* rh*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

Execution of setup completed successfully



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

2.2.5. Upgrading the Red Hat Virtualization Manager from 4.2 to 4.3

You need to be logged into the machine that you are upgrading.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to restore your Red Hat Virtualization Manager installation to its previous state. For this reason, do not remove the previous version's repositories until after the upgrade is complete. If the upgrade fails, the **engine-setup** script explains how to restore your installation.

Procedure

1. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

- Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

- Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

- Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms
```

- Update the base operating system:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

The Manager is now upgraded to version 4.3.

You can now update the hosts.

2.2.6. Updating All Hosts in a Cluster

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See [oVirt Cluster Upgrade](#) for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.

- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
6. Review the summary of the hosts and virtual machines that are affected.
7. Click **Upgrade**.
8. A cluster upgrade status screen displays with a progress bar showing the percentage of completion, and a list of steps in the upgrade process that have completed. You can click **Go to**

Event Log to open the log entries for the upgrade. Closing this screen does not interrupt the upgrade process.

You can track the progress of host updates:

- in the **Compute → Clusters** view, the **Upgrade Status** column displays a progress bar that displays the percentage of completion.
- in the **Compute → Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

2.2.7. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to 4.6 on the virtual machine and verifying the network connection. If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

2.2.8. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute → Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

2.2.9. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

2.2.10. Replacing SHA-1 Certificates with SHA-256 Certificates

Red Hat Virtualization 4.4 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures.



WARNING

Do *NOT* let certificates expire. If they expire, the environment becomes non-responsive and recovery is an error prone and time consuming process. For information on renewing certificates, see [Renewing certificates before they expire](#) in the *Administration Guide*.

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
```

```

subject="$(
  openssl \
    x509 \
    -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
    -noout \
    -subject \
    -nameopt compat \
  | sed \
    's;subject=\..*\);1;' \
)"
/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
  --name="${name}" \
  --password=mypass \ <1>
  --subject="${subject}" \
  --san=DNS:"${ENGINE_FQDN}" \
  --keep-key
done

```

Do not change this the password value.

- Restart the **httpd** service:

```
# systemctl restart httpd
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

- Log in to the Manager machine as the root user.
- Check whether **/etc/pki/ovirt-engine/openssl.conf** includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

- Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S)"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

- Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

- Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

- On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
      -nameopt compat \
    | sed \
      's;subject=\.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \ <1> \
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

Do not change this the password value.

- Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate

authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance** and **OK**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

CHAPTER 3. UPGRADING A STANDALONE MANAGER REMOTE DATABASE ENVIRONMENT

3.1. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM RED HAT VIRTUALIZATION 4.3 TO 4.4

Upgrading your environment from 4.3 to 4.4 involves the following steps:

Upgrade Considerations

- When planning to upgrade, see [Red Hat Virtualization 4.4 upgrade considerations and known issues](#).
- When upgrading from Open Virtual Network (OVN) and Open vSwitch (OvS) 2.11 to OVN 2021 and OvS 2.15, the process is transparent to the user as long as the following conditions are met:
 - The Manager is upgraded first.
 - The `ovirt-provider-ovn` security groups must be disabled, before the host upgrade, for all OVN networks that are expected to work between hosts with OVN/OvS version 2.11.
 - The hosts are upgraded to match OVN version 2021 or higher and OvS version 2.15. You must complete this step in the Administration Portal, so you can properly reconfigure OVN and refresh the certificates.
 - The host is rebooted after an upgrade.



NOTE

To verify whether the provider and OVN were configured successfully on the host, check the **OVN configured** flag on the **General** tab for the host. If the **OVN Configured** is set to **No**, click **Management → Refresh Capabilities**. This setting is also available in the REST API. If refreshing the capabilities fails, you can configure OVN by reinstalling the host from Manager 4.4 or higher.

1. [Make sure you meet the prerequisites, including enabling the correct repositories.](#)
2. [Use the Log Collection Analysis tool and Image Discrepancies tool to check for issues that might prevent a successful upgrade.](#)
3. [Update the 4.3 Manager to the latest version of 4.3.](#)
4. [Upgrade the Manager from 4.3 to 4.4.](#)
5. [Upgrade the remote Data Warehouse service and database.](#)
6. [Migrate hosts and virtual machines while reducing virtual machine downtime.](#)
7. [Optional: Upgrade RHVH while preserving local storage.](#)
8. [Update the compatibility version of the clusters.](#)
9. [Reboot any running or suspended virtual machines to update their configuration.](#)

10. [Update the compatibility version of the data centers.](#)

3.1.1. Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- When upgrading Red Hat Virtualization Manager, it is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

3.1.2. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

3.1.3. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

3.1.3.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.



NOTE

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```

Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
  storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
  storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  No discrepancies found

```

You can now update the Manager to the latest version of 4.3.

3.1.4. Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.4.

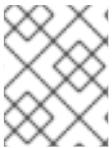
3.1.5. Upgrading the Red Hat Virtualization Manager from 4.3 to 4.4

Red Hat Virtualization Manager 4.4 is only supported on Red Hat Enterprise Linux versions 8.2 to 8.6. You need to do a clean installation of Red Hat Enterprise Linux 8.6 and Red Hat Virtualization Manager 4.4, even if you are using the same physical machine that you use to run RHV Manager 4.3.

The upgrade process requires restoring Red Hat Virtualization Manager 4.3 backup files onto the Red Hat Virtualization Manager 4.4 machine.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3.
- All virtual machines in the environment must have the cluster compatibility level set to version 4.3.
- If you use an external CA to sign HTTPS certificates, follow the steps in [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*. The backup and restore include the 3rd-party certificate, so you should be able to log in to the Administration portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works. See [BZ#1313379](#) for more information.



NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Procedure

1. Log in to the Manager machine.
2. Back up the Red Hat Virtualization Manager 4.3 environment.

```
# engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
```

3. Copy the backup file to a storage device outside of the RHV environment.
4. Install Red Hat Enterprise Linux 8.6. See [Performing a standard RHEL installation](#) for more information.
5. Complete the steps to install Red Hat Virtualization Manager 4.4, including running the command **yum install rhvm**, but do not run **engine-setup**. See one of the *Installing Red Hat Virtualization* guides for more information.
6. Copy the backup file to the Red Hat Virtualization Manager 4.4 machine and restore it.

```
# engine-backup --mode=restore --file=backup.bck --provision-all-databases
```



NOTE

If the backup contained grants for extra database users, this command creates the extra users with random passwords. You must change these passwords manually if the extra users require access to the restored system. See <https://access.redhat.com/articles/2686731>.

7. Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

8. Install optional extension packages if they were installed on the Red Hat Virtualization Manager 4.3 machine.

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc
```



NOTE

The **ovirt-engine-extension-aaa-ldap** is deprecated. For new installations, use Red Hat Single Sign On. For more information, see [Installing and Configuring Red Hat Single Sign-On](#) in the *Administration Guide*.



NOTE

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

9. Configure the Manager by running the **engine-setup** command:

```
# engine-setup
```

10. Decommission the Red Hat Virtualization Manager 4.3 machine if a different machine is used for Red Hat Virtualization Manager 4.4. Two different Managers must not manage the same hosts or storage.

The Red Hat Virtualization Manager 4.4 is now installed, with the cluster compatibility version set to 4.2 or 4.3, whichever was the preexisting cluster compatibility version.

Now you need to upgrade the remote databases in your environment.



NOTE

'engine-setup' also stops the Data Warehouse service on the remote Data Warehouse machine.

If you intend to postpone the next parts of this procedure, log in to the Data Warehouse machine and start the Data Warehouse service:

```
# systemctl start ovirt-engine-dwhd.service
```

Additional resources

- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

3.1.6. Upgrading the remote Data Warehouse service and database

Run this procedure on the remote machine with the Data Warehouse service and database.

Notice that part of this procedure requires you to install Red Hat Enterprise Linux 8.6, or Red Hat Virtualization Host 4.4.

Prerequisites

- You are logged in to the Data Warehouse machine.
- A storage device outside the RHV environment.

Procedure

1. Back up the Data Warehouse machine.



NOTE

Grafana is not supported on RHV 4.3, but on RHV 4.4, this command also includes the Grafana service and the Grafana database.

```
# engine-backup --file=<backupfile>
```

2. Copy the backup file to a storage device.
3. Stop and disable the Data Warehouse service:

```
# systemctl stop ovirt-engine-dwhd  
# systemctl disable ovirt-engine-dwhd
```

4. Reinstall the Data Warehouse machine with Red Hat Enterprise Linux 8.6, or Red Hat Virtualization Host 4.4.
5. Prepare a PostgreSQL database. For information, see [Preparing a Remote PostgreSQL Database](#) in *Installing Red Hat Virtualization as a standalone Manager with remote databases*.
6. Enable the correct repositories on the server and install the Data Warehouse service. For detailed instructions, see [Installing and Configuring Data Warehouse on a Separate Machine](#) for Red Hat Virtualization 4.4. Complete the steps in that procedure up to and including the **dnf install ovirt-engine-dwh-setup** command. Then continue to the next step in this procedure.
7. Copy the backup file from the storage device to the Data Warehouse machine.
8. Restore the backup file:

```
# engine-backup --mode=restore --file=backup.bck --provision-all-databases
```

9. On the Data Warehouse machine, run the **engine-setup** command:

```
# engine-setup
```

10. On the Manager machine, restart the Manager to connect it to the Data Warehouse database:

```
# systemctl restart ovirt-engine
```

Additional resources

- [Performing a standard RHEL installation](#)

- [Installing Hosts for Red Hat Virtualization](#) in *Installing Red Hat Virtualization as a standalone Manager with remote databases*

You can now update the hosts.

3.1.7. Migrating hosts and virtual machines from RHV 4.3 to 4.4

You can migrate hosts and virtual machines from Red Hat Virtualization 4.3 to 4.4 such that you minimize the downtime of virtual machines in your environment.

This process requires migrating all virtual machines from one host so as to make that host available to upgrade to RHV 4.4. After the upgrade, you can reattach the host to the Manager.



WARNING

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.



NOTE

CPU-passthrough virtual machines might not migrate properly from RHV 4.3 to RHV 4.4.

RHV 4.3 and RHV 4.4 are based on RHEL 7 and RHEL 8, respectively, which have different kernel versions with different CPU flags and microcodes. This can cause problems in migrating CPU-passthrough virtual machines.

Prerequisites

- Hosts for RHV 4.4 require Red Hat Enterprise Linux versions 8.2 to 8.6. A clean installation of Red Hat Enterprise Linux 8.6, or Red Hat Virtualization Host 4.4 is required, even if you are using the same physical machine that you use to run hosts for RHV 4.3.
- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the hosts belong is set to 4.2 or 4.3. All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.

Procedure

1. Pick a host to upgrade and migrate that host's virtual machines to another host in the same cluster. You can use Live Migration to minimize virtual machine downtime. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide*.
2. Put the host into maintenance mode and remove the host from the Manager. For more information, see [Removing a Host](#) in the *Administration Guide*.

3. Install Red Hat Enterprise Linux 8.6, or RHVH 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
4. Install the appropriate packages to enable the host for RHV 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
5. Add this host to the Manager, assigning it to the same cluster. You can now migrate virtual machines onto this host. For more information, see [Adding Standard Hosts to the Manager](#) in one of the *Installing Red Hat Virtualization* guides.

Repeat these steps to migrate virtual machines and upgrade hosts for the rest of the hosts in the same cluster, one by one, until all are running Red Hat Virtualization 4.4.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)
- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

3.1.8. Upgrading RHVH while preserving local storage

Environments with local storage cannot migrate virtual machines to a host in another cluster because the local storage is not shared with other storage domains. To upgrade RHVH 4.3 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain in the 4.4 environment, and import the previous local storage into the new domain.

Prerequisites

- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the host belongs is set to 4.2 or 4.3.

Procedure

1. Ensure that the local storage on the RHVH 4.3 host's local storage is in maintenance mode before starting this process. Complete these steps:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the **Details** pane and select the storage domain in the results list.
 - c. Click **Maintenance**.
2. Reinstall the Red Hat Virtualization Host, as described in [Installing Red Hat Virtualization Host](#) in the *Installation Guide*.



IMPORTANT

When selecting the device on which to install RHVH from the **Installation Destination** screen, do not select the device(s) storing the virtual machines. Only select the device where the operating system should be installed.

If you are using Kickstart to install the host, ensure that you preserve the devices containing the virtual machines by adding the following to the Kickstart file, replacing ``device`` with the relevant device.

```
# clearpart --all --drives=device
```

For more information on using Kickstart, see [Kickstart references](#) in *Red Hat Enterprise Linux 8 Performing an advanced RHEL installation*.

3. On the reinstalled host, create a directory, for example **/data** in which to recover the previous environment.

```
# mkdir /data
```

4. Mount the previous local storage in the new directory. In our example, **/dev/sdX1** is the local storage:

```
# mount /dev/sdX1 /data
```

5. Set the following permissions for the new directory.

```
# chown -R 36:36 /data
# chmod -R 0755 /data
```

6. Red Hat recommends that you also automatically mount the local storage via **/etc/fstab** in case the server requires a reboot:

```
# blkid | grep -i sdX1
/dev/sdX1: UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" TYPE="ext4"
# vi /etc/fstab
UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" /data ext4 defaults 0 0
```

7. In the Administration Portal, create a data center and select **Local** in the **Storage Type** drop-down menu.
8. Configure a cluster on the new data center. See [Creating a New Cluster](#) in the *Administration Guide* for more information.
9. Add the host to the Manager. See [Adding Standard Hosts to the Red Hat Virtualization Manager](#) in one of the *Installing Red Hat Virtualization* guides for more information.
10. On the host, create a new directory that will be used to create the initial local storage domain. For example:

```
# mkdir -p /localfs
# chown 36:36 /localfs
# chmod -R 0755 /localfs
```

11. In the Administration Portal, open the **Storage** tab and click **New Domain** to create a new local storage domain.
12. Set the name to **localfs** and set the path to **/localfs**.
13. Once the local storage is active, click **Import Domain** and set the domain's details. For example, define **Data** as the name, **Local on Host** as the storage type and **/data** as the path.
14. Click **OK** to confirm the message that appears informing you that storage domains are already attached to the data center.
15. Activate the new storage domain:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the details pane and select the new data storage domain in the results list.
 - c. Click **Activate**.
16. Once the new storage domain is active, import the virtual machines and their disks:
 - a. In the **Storage** tab, select **data**.
 - b. Select the **VM Import** tab in the details pane, select the virtual machines and click **Import**. See [Importing Virtual Machines from a Data Domain](#) in the *Virtual Machine Management Guide* for more details.
17. Once you have ensured that all virtual machines have been successfully imported and are functioning properly, you can move **localfs** to maintenance mode.
18. Click the **Storage** tab and select **localfs** from the results list.
 - a. Click the **Data Center** tab in the details pane.
 - b. Click Maintenance, then click **OK** to move the storage domain to maintenance mode.
 - c. Click **Detach**. The Detach Storage confirmation window opens.
 - d. Click **OK**.

You have now upgraded the host to version 4.4, created a new local storage domain, and imported the 4.3 storage domain and its virtual machines.

You can now update the cluster compatibility version.

3.1.9. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to 4.6 on the virtual machine and verifying the network connection. If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

You can now update the cluster compatibility version for virtual machines in the cluster.

3.1.10. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now update the data center compatibility version.

3.1.11. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

3.2. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM RED HAT VIRTUALIZATION 4.2 TO 4.3

Upgrading your environment from 4.2 to 4.3 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool and Image Discrepancies tool to check for issues that might prevent a successful upgrade](#)
3. [Update the 4.2 Manager to the latest version of 4.2](#)
4. [Upgrade the database from PostgreSQL 9.5 to 10.0](#)
5. [Upgrade the Manager from 4.2 to 4.3](#)
6. [Update the hosts](#)
7. [Update the compatibility version of the clusters](#)

8. [Reboot any running or suspended virtual machines to update their configuration](#)
9. [Update the compatibility version of the data centers](#)
10. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

3.2.1. Prerequisites

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).
- When upgrading Red Hat Virtualization Manager, it is recommended that you use one of the existing hosts. If you decide to use a new host, you must assign a unique name to the new host and then add it to the existing cluster before you begin the upgrade procedure.

3.2.2. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

3.2.3. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

3.2.3.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.



NOTE

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
  storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
  storage(5424252928) and on DB(5424254976)

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  No discrepancies found
```

You can now update the Manager to the latest version of 4.2.

3.2.4. Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

- Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

3.2.5. Upgrading remote databases from PostgreSQL 9.5 to 10

Red Hat Virtualization 4.3 uses PostgreSQL 10 instead of PostgreSQL 9.5. If your databases are installed locally, the upgrade script automatically upgrades them from version 9.5 to 10. However, if

either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:

- When upgrading the Manager database, stop the **ovirt-engine** service on the Manager machine:

```
# systemctl stop ovirt-engine
```

- When upgrading the Data Warehouse database, stop the **ovirt-engine-dwhd** service on the Data Warehouse machine:

```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 10 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.3-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 10 packages:

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.5 service:

```
# systemctl stop rh-postgresql95-postgresql  
# systemctl disable rh-postgresql95-postgresql
```

5. Upgrade the PostgreSQL 9.5 database to PostgreSQL 10:

```
# scl enable rh-postgresql10 -- postgresql-setup --upgrade-from=rh-postgresql95-postgresql  
--upgrade
```

6. Start and enable the **rh-postgresql10-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql10-postgresql.service  
# systemctl enable rh-postgresql10-postgresql.service  
# systemctl status rh-postgresql10-postgresql.service
```

Ensure that you see output similar to the following:

```
rh-postgresql10-postgresql.service - PostgreSQL database server  
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql10-postgresql.service;  
enabled; vendor preset: disabled)  
Active: active (running) since ...
```

- Copy the **pg_hba.conf** client configuration file from the PostgreSQL 9.5 environment to the PostgreSQL 10 environment:

```
# cp -p /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-
postgresql10/lib/pgsql/data/pg_hba.conf
```

- Update the following parameters in **/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor=0.01
autovacuum_analyze_scale_factor=0.075
autovacuum_max_workers=6
maintenance_work_mem=65536
max_connections=150
work_mem = 8192
```

- Restart the PostgreSQL 10 service to apply the configuration changes:

```
# systemctl restart rh-postgresql10-postgresql.service
```

You can now upgrade the Manager to 4.3.

3.2.6. Upgrading the Red Hat Virtualization Manager from 4.2 to 4.3

Follow these same steps when upgrading any of the following:

- the Red Hat Virtualization Manager
- a remote machine with the Data Warehouse service

You need to be logged into the machine that you are upgrading.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to restore your Red Hat Virtualization Manager installation to its previous state. For this reason, do not remove the previous version's repositories until after the upgrade is complete. If the upgrade fails, the **engine-setup** script explains how to restore your installation.

Procedure

- Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
--enable=rhel-7-server-rhv-4.3-manager-rpms \
--enable=jb-eap-7.2-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

- Update the setup packages:

```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

- Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager, the remote database or remote service:

```
# engine-setup
```



NOTE

During the upgrade process for the Manager, the **engine-setup** script might prompt you to disconnect the remote Data Warehouse database. You must disconnect it to continue the setup.

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

- Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms
```

- Update the base operating system:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

The Manager is now upgraded to version 4.3.

3.2.6.1. Completing the remote Data Warehouse database upgrade

Complete these additional steps when upgrading a remote Data Warehouse database from PostgreSQL 9.5 to 10.

Procedure

- The **ovirt-engine-dwhd** service is now running on the Manager machine. If the **ovirt-engine-dwhd** service is on a remote machine, stop and disable the **ovirt-engine-dwhd** service on the Manager machine, and remove the configuration files that **engine-setup** created:

```
# systemctl stop ovirt-engine-dwhd
# systemctl disable ovirt-engine-dwhd
# rm -f /etc/ovirt-engine-dwh/ovirt-engine-dwhd.conf.d/*
```

-
- 2. Repeat the steps in [Upgrading the Manager to 4.3](#) on the machine hosting the **ovirt-engine-dwhd** service.

You can now update the hosts.

3.2.7. Updating All Hosts in a Cluster

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See [oVirt Cluster Upgrade](#) for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade

process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.

- **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to `cluster_maintenance` during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that are affected.
 7. Click **Upgrade**.
 8. A cluster upgrade status screen displays with a progress bar showing the percentage of completion, and a list of steps in the upgrade process that have completed. You can click **Go to Event Log** to open the log entries for the upgrade. Closing this screen does not interrupt the upgrade process.

You can track the progress of host updates:

- in the **Compute** → **Clusters** view, the **Upgrade Status** column displays a progress bar that displays the percentage of completion.
- in the **Compute** → **Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute** → **Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

3.2.8. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to

4.6 on the virtual machine and verifying the network connection.

If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

3.2.9. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.

**NOTE**

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

3.2.10. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

3.2.11. Replacing SHA-1 Certificates with SHA-256 Certificates

Red Hat Virtualization 4.4 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures.

**WARNING**

Do *NOT* let certificates expire. If they expire, the environment becomes non-responsive and recovery is an error prone and time consuming process. For information on renewing certificates, see [Renewing certificates before they expire](#) in the *Administration Guide*.

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, save a backup of the **/etc/ovirt-engine/engine.conf.d** and **/etc/pki/ovirt-engine** directories, and re-sign the certificates:

```
# . /etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
      -nameopt compat \
    | sed \
      's;subject=\.*)\;1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \ <1>
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

Do not change this the password value.

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

6. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
      -nameopt compat \
    | sed \
      's;subject=\.*)\;1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \ <1>
```

```
--subject="${subject}" \  
--san=DNS:${ENGINE_FQDN}" \  
--keep-key  
done
```

Do not change this the password value.

7. Restart the following services:

```
# systemctl restart httpd  
# systemctl restart ovirt-engine  
# systemctl restart ovirt-websocket-proxy  
# systemctl restart ovirt-imageio
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance** and **OK**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

CHAPTER 4. UPDATES BETWEEN MINOR RELEASES

4.1. UPDATING RED HAT VIRTUALIZATION BETWEEN MINOR RELEASES

To update from your current version of 4.4 to the latest version of 4.4, update the Manager, update the hosts, and then change the compatibility version for the cluster, virtual machines, and data center.



NOTE

If upgrading from version 4.4.9 to a later version fails on RHVH, run the **dnf reinstall redhat-virtualization-host-image-update** command to fix the issue.

Upgrade Considerations

- When planning to upgrade, see [Red Hat Virtualization 4.4 upgrade considerations and known issues](#).
- When upgrading from Open Virtual Network (OVN) and Open vSwitch (OvS) 2.11 to OVN 2021 and OvS 2.15, the process is transparent to the user as long as the following conditions are met:
 - The Manager is upgraded first.
 - The ovirt-provider-ovn security groups must be disabled, before the host upgrade, for all OVN networks that are expected to work between hosts with OVN/OvS version 2.11.
 - The hosts are upgraded to match OVN version 2021 or higher and OvS version 2.15. You must complete this step in the Administration Portal, so you can properly reconfigure OVN and refresh the certificates.
 - The host is rebooted after an upgrade.



NOTE

To verify whether the provider and OVN were configured successfully on the host, check the **OVN configured** flag on the **General** tab for the host. If the **OVN Configured** is set to **No**, click **Management → Refresh Capabilities**. This setting is also available in the REST API. If refreshing the capabilities fails, you can configure OVN by reinstalling the host from Manager 4.4 or higher.

4.1.1. Analyzing the Environment

It is recommended to run the **Log Collection Analysis** tool and the **Image Discrepancies** tool prior to performing updates and for troubleshooting. These tools analyze your environment for known issues that might prevent you from performing an update, and provide recommendations to resolve them.

4.1.2. Log Collection Analysis tool

Run the **Log Collection Analysis** tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them. The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

4.1.2.1. Monitoring snapshot health with the image discrepancies tool

The **RHV Image Discrepancies** tool analyzes image data in the Storage Domain and RHV Database. It alerts you if it finds discrepancies in volumes and volume attributes, but does not fix those discrepancies. Use this tool in a variety of scenarios, such as:

- Before upgrading versions, to avoid carrying over broken volumes or chains to the new version.
- Following a failed storage operation, to detect volumes or attributes in a bad state.
- After restoring the RHV database or storage from backup.
- Periodically, to detect potential problems before they worsen.
- To analyze a snapshot- or live storage migration-related issues, and to verify system health after fixing these types of problems.

Prerequisites

- **Required Versions:** this tool was introduced in RHV version 4.3.8 with **rhv-log-collector-analyzer-0.2.15-0.el7ev**.
- Because data collection runs simultaneously at different places and is not atomic, stop all activity in the environment that can modify the storage domains. That is, do not create or remove snapshots, edit, move, create, or remove disks. Otherwise, false detection of inconsistencies may occur. Virtual Machines can remain running normally during the process.

Procedure

1. To run the tool, enter the following command on the RHV Manager:

```
# rhv-image-discrepancies
```

2. If the tool finds discrepancies, rerun it to confirm the results, especially if there is a chance some operations were performed while the tool was running.



NOTE

This tool includes any Export and ISO storage domains and may report discrepancies for them. If so, these can be ignored, as these storage domains do not have entries for images in the RHV database.

Understanding the results

The tool reports the following:

- If there are volumes that appear on the storage but are not in the database, or appear in the database but are not on the storage.
- If some volume attributes differ between the storage and the database.

Sample output:

```
Checking storage domain c277ad93-0973-43d9-a0ca-22199bc8e801
  Looking for missing images...
  No missing images found
  Checking discrepancies between SD/DB attributes...
  image ef325650-4b39-43cf-9e00-62b9f7659020 has a different attribute capacity on
  storage(2696984576) and on DB(2696986624)
  image 852613ce-79ee-4adc-a56a-ea650dcb4cfa has a different attribute capacity on
  storage(5424252928) and on DB(5424254976)
```

```

Checking storage domain c64637b4-f0e8-408c-b8af-6a52946113e2
Looking for missing images...
No missing images found
Checking discrepancies between SD/DB attributes...
No discrepancies found

```

To update a standalone Manager, follow the standard procedure for minor updates:

4.1.3. Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4.



NOTE

If you are upgrading from RHV version 4.4.0 through 4.4.8 to RHV version 4.4.9 or later, you must add the EAP 7.4 channel to the list of subscription repositories **jb-eap-7.4-for-rhel-8-x86_64-rpms**, and following the upgrade, remove the **jb-eap-7.3-for-rhel-8-x86_64-rpms** from the list of subscription repositories.

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

**NOTE**

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```

**IMPORTANT**

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

4.1.4. Updating a Self-Hosted Engine

To update a self-hosted engine from your current version to the latest version, you must place the environment in global maintenance mode and then follow the standard procedure for updating between minor versions.

**NOTE**

Ensure the Manager has the correct repositories enabled. For the list of required repositories, see the section [Updating the Red Hat Virtualization Manager](#).

Enabling global maintenance mode

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in global maintenance mode before proceeding:

■

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in global maintenance mode.

Updating the Red Hat Virtualization Manager

Prerequisites

- **Ensure the Manager has the correct repositories enabled** For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4.



NOTE

If you are upgrading from RHV version 4.4.0 through 4.4.8 to RHV version 4.4.9 or later, you must add the EAP 7.4 channel to the list of subscription repositories **jb-eap-7.4-for-rhel-8-x86_64-rpms**, and following the upgrade, remove the **jb-eap-7.3-for-rhel-8-x86_64-rpms** from the list of subscription repositories.

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt\*setup\* rh\*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update --nobest
```

**IMPORTANT**

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#) .

**IMPORTANT**

If any kernel packages were updated:

- Disable global maintenance mode
- Reboot the machine to complete the update.

Related Information

[Disabling global maintenance mode](#)

Disabling global maintenance mode**Procedure**

- Log in to the Manager virtual machine and shut it down.
- Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

- Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```

**NOTE**

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

4.1.5. Updating All Hosts in a Cluster

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See [oVirt Cluster Upgrade](#) for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where

the hosts update quickly.

- **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to [cluster_maintenance](#) during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that are affected.
 7. Click **Upgrade**.
 8. A cluster upgrade status screen displays with a progress bar showing the percentage of completion, and a list of steps in the upgrade process that have completed. You can click **Go to Event Log** to open the log entries for the upgrade. Closing this screen does not interrupt the upgrade process.

You can track the progress of host updates:

- in the **Compute → Clusters** view, the **Upgrade Status** column displays a progress bar that displays the percentage of completion.
- in the **Compute → Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute → Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

You can now update the cluster compatibility version.

4.1.6. Changing the Cluster Compatibility Version

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.

Prerequisites

- To change the cluster compatibility level, you must first update all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Limitations

- Virtio NICs are enumerated as a different device after upgrading the cluster compatibility level to 4.6. Therefore, the NICs might need to be reconfigured. Red Hat recommends that you test the virtual machines before you upgrade the cluster by setting the cluster compatibility level to 4.6 on the virtual machine and verifying the network connection.
If the network connection for the virtual machine fails, configure the virtual machine with a custom emulated machine that matches the current emulated machine, for example `pc-q35-rhel8.3.0` for 4.5 compatibility version, before upgrading the cluster.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

You can now update the cluster compatibility version for virtual machines in the cluster.

4.1.7. Changing Virtual Machine Cluster Compatibility

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, or from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now update the data center compatibility version.

4.1.8. Changing the Data Center Compatibility Version

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.

Prerequisites

- To change the data center compatibility level, you must first update the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

You can also update hosts individually:

4.1.9. Updating Individual Hosts

Use the host upgrade manager to update individual hosts directly from the Administration Portal.



NOTE

The upgrade manager only checks hosts with a status of **Up** or **Non-operational**, but not **Maintenance**.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.

- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure

1. Ensure that the correct repositories are enabled. To view a list of currently enabled repositories, run **dnf repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
  --enable=rhel-8-for-x86_64-baseos-eus-rpms \
  --enable=rhel-8-for-x86_64-appstream-eus-rpms \
  --enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
  --enable=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms

# subscription-manager release --set=8.6
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Installation** → **Check for Upgrade** and click **OK**.
Open the **Notification Drawer** () and expand the **Events** section to see the result.
4. If an update is available, click **Installation** → **Upgrade**.
5. Click **OK** to update the host. Running virtual machines are migrated according to their migration policy. If migration is disabled for any virtual machines, you are prompted to shut them down. The details of the host are updated in **Compute** → **Hosts** and the status transitions through these stages:

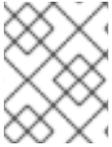
Maintenance > **Installing** > **Reboot** > **Up**



NOTE

If the update fails, the host's status changes to **Install Failed**. From **Install Failed** you can click **Installation** → **Upgrade** again.

Repeat this procedure for each host in the Red Hat Virtualization environment.



NOTE

You should update the hosts from the Administration Portal. However, you can update the hosts using **dnf upgrade** instead.

4.1.10. Manually Updating Hosts

CAUTION

This information is provided for advanced system administrators who need to update hosts manually, but Red Hat does not support this method. The procedure described in this topic does not include important steps, including certificate renewal, assuming advanced knowledge of such information. Red Hat supports updating hosts using the Administration Portal. For details, see [Updating individual hosts](#) or [Updating all hosts in a cluster](#) in the *Administration Guide*.

You can use the **dnf** command to update your hosts. Update your systems regularly, to ensure timely application of security and bug fixes.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure

1. Ensure the correct repositories are enabled. You can check which repositories are currently enabled by running **dnf repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
--enable=rhel-8-for-x86_64-baseos-eus-rpms \
--enable=rhel-8-for-x86_64-appstream-eus-rpms \
--enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
--enable=advanced-virt-for-rhel-8-x86_64-rpms \
```

```
--enable=fast-datapath-for-rhel-8-x86_64-rpms
# subscription-manager release --set=8.6
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Management** → **Maintenance** and **OK**.
4. For Red Hat Enterprise Linux hosts:

- a. Identify the current version of Red Hat Enterprise Linux:

```
# cat /etc/redhat-release
```

- b. Check which version of the redhat-release package is available:

```
# dnf --refresh info --available redhat-release
```

This command shows any available updates. For example, when upgrading from Red Hat Enterprise Linux 8.2.z to 8.3, compare the version of the package with the currently installed version:

```
Available Packages
Name      : redhat-release
Version   : 8.3
Release   : 1.0.el8
...
```

CAUTION

The Red Hat Enterprise Linux Advanced Virtualization module is usually released later than the Red Hat Enterprise Linux y-stream. If no new Advanced Virtualization module is available yet, or if there is an error enabling it, stop here and cancel the upgrade. Otherwise you risk corrupting the host.

- c. If the Advanced Virtualization stream is available for Red Hat Enterprise Linux 8.3 or later, reset the **virt** module:

```
# dnf module reset virt
```



NOTE

If this module is already enabled in the Advanced Virtualization stream, this step is not necessary, but it has no negative impact.

You can see the value of the stream by entering:

```
# dnf module list virt
```

- d. Enable the **virt** module in the Advanced Virtualization stream with the following command:
 - For RHV 4.4.2:
 -

```
# dnf module enable virt:8.2
```

- For RHV 4.4.3 to 4.4.5:

```
# dnf module enable virt:8.3
```

- For RHV 4.4.6 to 4.4.10:

```
# dnf module enable virt:av
```

- For RHV 4.4 and later:

```
# dnf module enable virt:rhel
```



NOTE

Starting with RHEL 8.6 the Advanced virtualization packages will use the standard **virt:rhel** module. For RHEL 8.4 and 8.5, only one Advanced Virtualization stream is used, **rhel:av**.

5. Enable version 14 of the **nodejs** module:

```
# dnf module -y enable nodejs:14
```

6. Update the host:

```
# dnf upgrade --nobest
```

7. Reboot the host to ensure all updates are correctly applied.



NOTE

Check the `imgbased` logs to see if any additional package updates have failed for a Red Hat Virtualization Host. If some packages were not successfully reinstalled after the update, check that the packages are listed in `/var/imgbased/persisted-rpms`. Add any missing packages then run **rpm -Uvh /var/imgbased/persisted-rpms/***.

Repeat this process for each host in the Red Hat Virtualization environment.

APPENDIX A. UPDATING THE LOCAL REPOSITORY FOR AN OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION

If your Red Hat Virtualization Manager is hosted on a machine that receives packages via FTP from a local repository, you must regularly synchronize the repository to download package updates from the Content Delivery Network, then update or upgrade that machine. Updated packages address security issues, fix bugs, and add enhancements.

1. On the system hosting the repository, synchronize the repository to download the most recent version of each available package:

```
# reposync --newest-only -p /var/ftp/pub/rhevrepo
```

This command might download a large number of packages, and take a long time to complete.

2. Ensure that the repository is available on the Manager machine, and then update or upgrade the machine.

APPENDIX B. INSTALLING RHV HYPERVISORS FROM A LOCAL REPOSITORY

If your system uses a private Red Hat Virtualization (RHV) environment, but without Red Hat Satellite, you might need to install RHV hypervisors (RHV-H) from a repository hosted on a local RHEL system instead of the Red Hat hosted Content Delivery Network (CDN).

Procedure

1. On the system hosting the offline repository, create a file named `/etc/yum.repos.d/rhvh-mirror.repo` with contents similar to the lines that follow:

```
[rhvh-4-for-rhel-8-x86_64-rpms]
name = Red Hat Virtualization Host for RHEL 8 x86_64 (RPMs)
baseurl = https://cdn.redhat.com/content/dist/layered/rhel8/x86_64/rhvh/4/os
enabled = 0
gpgcheck = 1
gpgkey = file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
sslverify = 1
sslcacert = /etc/rhsm/ca/redhat-uep.pem
metadata_expire = 86400
enabled_metadata = 1
sslclientcert =
sslclientkey =
```

You must populate the `sslclientcert` and `sslclientkey` fields with full path names to the correct files containing the appropriate certificate and key. The `/etc/pki/entitlement` directory contains one or more pairs of certificate and key files, but only one pair contains the RHV-H entitlement you need.

2. To find the certificate file:
 - a. List all files in the `/etc/pki/entitlement` directory:

```
# ls -al /etc/pki/entitlement/
```

Output similar to the following is displayed:

```
total 836
drwxr-xr-x. 2 root root  202 May 28 15:18 .
drwxr-xr-x. 15 root root  208 Apr 23  2020 ..
-rw-r--r--. 1 root root  3243 May 28 15:18 4522783034260408538-key.pem
-rw-r--r--. 1 root root 152622 May 28 15:18 4522783034260408538.pem
-rw-r--r--. 1 root root  3243 May 28 15:18 5659494963772844103-key.pem
-rw-r--r--. 1 root root  343394 May 28 15:19 5659494963772844103.pem
-rw-r--r--. 1 root root  3243 May 23 13:19 645832581386032208-key.pem
-rw-r--r--. 1 root root  343389 May 23 13:19 645832581386032208.pem
#
```

- b. Use the `rct cat-cert` command on each certificate in order to find the one that contains the RHV-H entitlement:

```
# cd /etc/pki/entitlement/
# rct cat-cert 5659494963772844103.pem | grep rhvh/4/ | grep URL
```

Output similar to the following is displayed:

```
URL: /content/beta/rhel/server/7/$basearch/rhvh/4/os
URL: /content/dist/rhel/server/7/7Server/$basearch/rhvh/4/os
URL: /content/beta/layered/rhel8/x86_64/rhvh/4/os
URL: /content/dist/layered/rhel8/x86_64/rhvh/4/os
```

3. Identify the correct certificate and fill in the **sslclientcert** and **sslclientkey** values in the previously mentioned **.repo** file:

```
sslclientcert = /etc/pki/entitlement/5659494963772844103.pem
sslclientkey = /etc/pki/entitlement/5659494963772844103-key.pem
```

4. Run the **reposync** command in the appropriate directory:
 - a. Use the 'pwd' command to determine the correct path:

```
# pwd
```

Output similar to the following is displayed:

```
/home/test/rhvh-reposync
```

- b. Run the **reposync** command:

```
# reposync --repo rhvh-4-for-rhel-8-x86_64-rpms
```

Output similar to the following is displayed:

```
Updating Subscription Management repositories.
Red Hat Virtualization Host for RHEL 8 x86_64 (RPMs)           11 kB/s | 4.0 kB
00:00
Red Hat Virtualization Host for RHEL 8 x86_64 (RPMs)         272 kB/s | 291
kB   00:01
.
.
.
(193/194): redhat-virtualization-host-image-update-4.4.5-20210330.0.el8_3.noarc 5.4
MB/s | 822 MB   02:30
(194/194): rhvm-appliance-4.4-20210310.0.el8ev.x86_64.rpm    5.6 MB/s |
1.5 GB   04:34
```

5. Check the certificate and key file pairs each time you run the **reposync** command because the Subscription Manager subsystem periodically regenerates them.

APPENDIX C. LEGAL NOTICE

Copyright © 2022 Red Hat, Inc.

Licensed under the ([Creative Commons Attribution–ShareAlike 4.0 International License](#)). Derived from documentation for the ([oVirt Project](#)). If you distribute this document or an adaptation of it, you must provide the URL for the original version.

Modified versions must remove all Red Hat trademarks.

Red Hat, Red Hat Enterprise Linux, the Red Hat logo, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

Java® is a registered trademark of Oracle and/or its affiliates.

XFS® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.